## REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

### Amendments to the Specification

The specification is amended on page 3 as suggested by the Examiner to clarify that the message and not the private key can be recovered using the public key. No new subject matter is believed to have been added by way of this amendment.

### Amendments to the Claims

Claim 1 is amended to clarify that the public key and not the private key is what is available to the other of the pair of correspondents, and to better reflect how the first, intermediate and second signature components are computed. Applicant notes that the expression "in which the plaintext is hidden" has been clarified in claim 1 to indicate that the component *c* is computed as a function of the bit string H wherein the bit string H is hidden in *c* and thus *c* is other than H itself. Claim 1 is also amended replacing "by including" with "containing" to clarify that the signature (s, c, V) contains the components s, c and the bit string V as discrete components. As suggested by the Examiner, "bitstring" on line 7 (now line 8) has been replaced with "bit string".

Claim 7 is amended to indicate that the purported signer is in a data transmission system, consistent with the terminology used in claim 1, and to add a step of verifying the message if the predetermined characteristic is present. Claim 7 is also amended clarifying that the signature contains a first component computed as a function of H where H is encrypted therein and the bit string V as a second component. The first step in claim 7 is amended indicating that a value is generated by combining the first component with the bit string V and the second step is amended accordingly, indicating that the bit string H is recovered from the value rather than "said combination".

Claims 8 and 10 are amended consistent with the terminology of amended claim 7. Claim 11 is amended replacing "formed" with "computed" on line 2.

Claim 12 is amended to clarify that the function is encryption with an "encryption key" that a "decryption key" is computable from information available in the signature, and that the complementary function is decryption with the decryption key. Support for these amendments to

claim 12 can be found on page 4, line 34 to page 6 line 9. Claim 13 is amended to clarify that the encryption key is a "short term key" derived from a "random integer" thereby removing reference to a public and private key pair. Support for these amendments can be found on page 4, lines 30-32.

No new subject matter is believed to have been added by way of these amendments.

**Claim Objections**

As noted above, "bitstring" has been replaced by "bit string" as suggested by the Examiner.

**Objections to the Specification**

As noted above, page 3 has been amended to clarify that the message and not the private key is recoverable using the public key.

**Claim Rejections – 35 U.S.C. 112**

Claims 1-13 have been rejected under 35 U.S.C. 112, second paragraph as being indefinite. Applicant believes that the amendments described above overcome the Examiner's rejections as explained below.

1. Claim 1 is amended to clarify that the public key is available to the other correspondent.
2. In claim 1, the expression "in which the plaintext is hidden" has been clarified in line 9 as discussed above and removed from line 15. Accordingly, this rejection is believed to have been overcome.
3. Claim 1 is amended to clarify that the bit string V is available from the signature (s,c,V) as an input, which is believed to address the Examiner's concern regarding this limitation.
4. In claim 7, the expression "said components" has been removed thus this rejection is thereby rendered moot.
5. The expression "said one component" is no longer used in claim 7. Applicant notes that previous "one component" is now referred to as a "first component". Therefore, Applicant believes that this rejection is thereby rendered moot.

6. As noted above, "said combination" has been replaced with "said value" and the first step of claim 7 indicates that "a value" is generated. Applicant believes that such an amendment overcomes this rejection.
7. As discussed above, claims 12 and 13 have been amended to distinguish between the encryption key used with the function and the decryption key that is computable from information available in the signature. This is exemplified in the description in the passage cited above. Applicant notes that, e.g. a symmetric key encryption algorithm uses the same key for encryption and decryption and believes that by removing reference to a public/private key pair in claim 13, this is clarified. Claim 13 now defines the encryption key as being a short term key that is derived from a random integer, the random integer also being used in the provision of the second component. This is clearly supported in the passage cited above.
8. As noted above, claim 12 is amended to clarify that the decryption key is computable from information available in the signature as exemplified in the description.
9. By virtue of the above, all claims not discussed are believed to comply as a result their respective dependencies.

In view of the above, Applicant believes that claims 1-13 fully comply with 35 U.S.C. 112, second paragraph.

**Claim Rejections – 35 U.S.C. 101**

Claims 7-8 have been rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Applicant respectfully traverses the rejections as follows.

Firstly, Applicant notes that verifying a signature based on the required redundancy is only a preferred implementation. Claim 7 specifies that the recovered plaintext be examined for a predetermined characteristic, which may include checking the redundancy but should not be limited to such. Applicant advises that the description relied on by the Examiner does not specify that checking the redundancy is the only characteristic but simply provides this as a practical implementation and example thereof.

Secondly, as noted above, claim 7 is amended to include the step of verifying the message if the predetermined characteristic is present. Clearly claim 7 involves a useful and tangible result, namely where the message is verified if a predetermined characteristic in the

recovered plaintext is present. Moreover, the method of claim 7 has a practical application in data transmission systems (clarified by way of amendment) and in particular, as admitted by the Examiner, to verifying a plaintext message.

Accordingly, Applicant believes that amended claim 7 clearly defines all the steps required to accomplish a verification and provides a concrete, useful and tangible result. Claim 7 is directed to a practical application in cryptographic systems and, as such is believed to constitute statutory subject matter. Therefore, Applicant believes that claims 7-8 comply with 35 U.S.C. 101.

**Claim Rejections – 35 U.S.C. 102**

Claims 1, 7 and 8 have been rejected under 35 U.S.C. 102(a) as being anticipated by ISO/IEC 9796-2 (ISO2). Applicant respectfully traverses the rejections as follows.

As previously argued, claim 1 recites a step of forming a signature (s,c,V) where the components in the signature are discrete signature components. Although Applicant believes that claim 1 as it was formerly recited clearly indicated that the components s, c and V were discrete components, as noted above, claim 1 has been amended replacing "by including" with "containing". Applicant believes that this amendment serves to address the Examiner's concern regarding the use of the expression "including".

The passage in ISO2 relied upon by the Examiner teaches a message allocation scheme and subsequent signature production, namely in sections 6.3.2 and 6.4 on page 5. In this passage, a message M is allocated in parts $M_r$ and $M_n$. An intermediate string *Si* is formed, in part, with a number of bits representing $M_r$. The string *Si* is processed to generate a recoverable string *Sr*, which is then transformed into the signature $\Sigma$. As set forth in section 6.4, the signed message includes $\Sigma$ and, where partial recovery is used, is provided together with $M_n$.

Clearly, ISO2 does not teach forming a signature that has components that are equivalent to (s,c,V). Firstly, ISO2 does not form a signature with three distinct components. Secondly, even if one were to equate component *c* in claim 1 to *Si* in ISO2, *Si* is then processed to arrive at $\Sigma$ and is not provided as a component itself. Thirdly, there is no intermediate component equivalent to *c'* recited in claim 1. In ISO2, *Si* is processed to obtain *Sr*, however, there is no mention of combining *Si* with $M_n$ at this stage. The Examiner believes $M_n$ to be equivalent to V in claim 1 and thus to be equivalent to claim 1, ISO2 must teach a combination of *Si* and $M_n$.

ISO2 is entirely silent in that regard. In claim 1, the component *s* is derived from the intermediate component *c'*. If no intermediate component *c'* exists in ISO2 then clearly there also exists no equivalent to *s* in ISO2.

Finally, it seems that the Examiner equates $\Sigma$ to an arbitrary derivation of *s* and *c* in claim 1 (which is in fact not recited) and that the use of the term "including" means that any such arbitrary derivation of equivalent components is taught by $\Sigma$. Not only does amended claim 1 clearly specify three discrete components, but, as discussed, $\Sigma$ is not derived from an equivalent to *c'* or *s*. Applicant believes that the Examiner has read too much into ISO2. However, Applicant also believes that amended claim 1 addresses the Examiner's concern regarding the use of the term "including" which is believed to place claim 1 in a better form for reconsideration. Moreover, in light of the arguments presented above, Applicant believes that even the previous language used in claim 1 is not anticipated by ISO2 for at least the reason that there is no teaching of an equivalent to the signature component *c'*.

Accordingly, Applicant believes that ISO2 fails to teach every element of claim 1 and, as such ISO2 cannot anticipate.

Regarding claim 7, amendments have been made to clarify the steps recited. In particular, the first step is amended to indicate that a value is generated by combining the first component with the bit string V. The Examiner believes that sections 6.3.3-6.4 and Table 1 of ISO2 teaches such a step. However, in these steps, the signature preparation is actually being performed, not the verification. It is clearly stated that "the signature shall be....or $\Sigma$ together with $M_n$ in the case of partial recovery." This is not a step of generating a value by combining such elements, but rather is the formation of the message having the elements as components in the signature. In any case, as noted above, $\Sigma$ cannot be considered equivalent to *c* but at most could be considered a derivation of a string that includes a component similar to *c* (e.g. *Si*).

Therefore, in order for the scheme in ISO2 to be equivalent to the step of generating a value in claim 7, $\Sigma$ would have to be disassembled and then combined with $M_n$, which is simply not shown. Moreover, the step of combining in claim 7 is performed in a verification process and not in a signature generation process. Applicant believes that the Examiner has not fully considered the actual execution of each portion of ISO2 that has been relied upon, but has instead pieced together steps from both the signature formation and verification protocols taught in ISO2.

Therefore, ISO2 does not teach a step of generating a value by combining a first component with a plaintext bit string. For at least that reason, ISO2 cannot anticipate claim 7.

Since Applicant is believed to have shown that ISO2 does not include a step of generating a value that is such a combination, ISO2 cannot teach a step of recovering a bit string H from the combination.

Clearly, ISO2 does not teach an equivalent method to claim 7 since it does not even teach a single equivalent step. Therefore, Applicant respectfully submits that ISO2 cannot anticipate claim 7. Claim 8 is believed to be distinguished by virtue of its dependency on claim 7.

**Claim Rejections – 35 U.S.C. 103**

Claims 1, 6 and 11-13 have been rejected under 35 U.S.C. 103(1) as being unpatentable over McCollom (EP 0918274) in view of allegedly admitted prior art. Applicant respectfully traverses the rejections as follows.

The Examiner believes that McCollom teaches every step in claim 1 with the exception of teaching forming a signature with a set of discrete signature components as recited.

Firstly, if Examiner admits that McCollom does not provide such discrete signature components, Applicant is unclear why this distinction in claim 1 is not clear to the Examiner when rejecting claim 1 in view of ISO2. It seems to Applicant that the Examiner has applied the same logic in applying both references (ISO2 and McCollom) but has utilized a different interpretation of claim 1 in each rejection, which is entirely improper. If claim 1 is clear enough that the Examiner is able to determine that McCollom does not teach forming a signature from discrete components, then Applicant believes that claim 1 is clear enough to warrant the same interpretation in view of ISO2. As a result, ISO2 should have never been cited as it has, since it appears to have been cited for the same reasons that McCollom was cited in a previous office action.

Secondly, as previously argued, not only does McCollom not teach forming a signature with a set of discrete components, McCollom does not compute the same components as recited in claim 1.

McCollom teaches a method for securing a data signal having a plurality of signal components. One of the signal components is signed and combined with another signal component. The combined signal is then encrypted and a signature of the encrypted signal is

generated to produce an encrypted second signal signature at an output fingerprint. (see col. 4, lines 34-56)

Clearly McCollom does not teach forming a signature from two signature components and a plaintext bit string to create an output signature as recited in claim 1. McCollom teaches generating an entirely different output, namely by encrypting a combined signal and signing the entire encrypted signal to create an output fingerprint. There is absolutely no suggestion in McCollum of sending a portion of a message "in the clear" as plaintext to be used as an input in the verification process. The signature produced by McCollom has a single component, namely the signed encrypted signal, not the three components recited in claim 1. Therefore, not only does McCollom not teach forming a signature with discrete components, but does not even teach equivalents to the three components recited in claim 1.

The alleged admitted prior art on page 1, last paragraph to page 2, line 9 cited by the Examiner in fact describes the ISO2 reference discussed in detail above. As discussed above, ISO2 does not teach providing a set of discrete components. In fact, the Examiner admits that ISO2 does not teach discrete components but relies on an overly broad interpretation of the term "including". Again, it is unclear how the Examiner can admit that ISO2 does not teach discrete components in one rejection and then clearly rely on it as teaching what is missing from McCollom in another rejection. Applicant believes that the Examiner has read too much into the references cited and in fact has provided a contradictory application of ISO2 in different rejections.

Therefore, for at least the reasons set forth above, Applicant respectfully submits that claim 1 clearly and patentably distinguishes over McCollom in view of ISO2 (a.k.a. "admitted prior art"). Claims 6, and 11-13 being ultimately dependent on claim 1 is also believed to distinguish over the combination of references.

Claims 2-5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom in view of ISO2 in further view of ISO/IEC 9697-1 (ISO1).

Claims 2-5 are ultimately dependent on claim 1. Applicant is believed to have shown that the combination of McCollom and ISO2 fails to teach what is recited in claim 1 and claim 1 is believed to be patentably distinguished thereover. Therefore, ISO1 must at least teach what is missing from McCollom and ISO2.

Applicant respectfully submits that ISO1 does not teach forming a signature from discrete

components as recited in claim 1 and, as such does not teach what is missing from McCollom and ISO2, but is entirely silent in that regard.

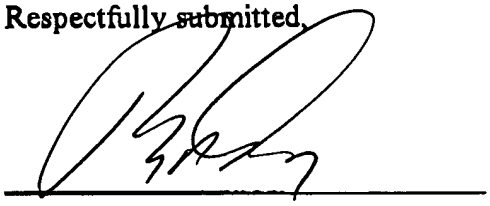
Accordingly, Applicant believes that claims 2-5 (being dependent on claim 1) clearly and patentably distinguish over McCollom in view of ISO2 in further view of ISO1.

**Summary**

In view of the foregoing, Applicants believe that all pending claims, namely claims 1-13 clearly and patentably distinguish over the references cited by the Examiner and are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Ralph A. Dowell
Attorney for Applicant
Registration No. 26,868

Date: 8-28, 2006